UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,501	11/02/2000	Oleg Rashkovskiy	ITL.0778US	8091

21906 7590 04/11/2007

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/706,501	RASHKOVSKIY ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,79-81 and 91-96* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,79-81, and 91-96* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 3/12/2007. Claims 1, 6, 27, 79, and 91 have been amended. Claims 29-78 and 82-90 have been cancelled.

Response to Arguments

Applicant's arguments with respect to claims 1-28, 79-81, and 91-96 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims are 1, 2-9, 21-28, 79, and 91 rejected under 35 U.S.C. 102(b) as being anticipated by Candelore et al., (U.S. Patent No. 6,061,449 and Candelore hereinafter).

Regarding claim 1, Candelore discloses an apparatus comprising:

a storage device to store an original content item in multiple blocks, each block containing at least a single byte (col. 1, lines 50-67 and col. 2, lines 1-7), the blocks stored in a logically linear fashion within the storage allocated for the content item (col.

19, lines 44-67 and col. 20, lines 1-5), a key generator (i.e., address generator) to generate a key according to [an identifier value of another apparatus](col. 24, lines 66-67 and col. 25, lines 1-20)(col. 26, lines 45-60 – wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit), a reorderer for reordering the blocks of an original content item according to [a symmetrical key K](i.e., a block-wise scrambling of N blocks according to an address data signal)(col. 26, lines 14-30), wherein the re-ordered blocks are stored in a non-linear fashion within the storage allocated for the re-ordered content item (col. 23, lines 63-67 and col. 24, lines 1-5).

Regarding claim 79, Candelore discloses a method comprising:

receiving from a first entity (i.e., the scrambling sender), reordered blocks of a content item, each block containing at least a single byte value, the bits within the blocks not reordered, the order of said reordered blocks different from the block order for the original content item (col. 3, lines 44-67),creating a block reordering structure within a second entity (i.e., the descrambling receiver), and accessing a block of the original content item by retrieving it from the reordered content item according to the block reordering structure (col. 26, lines 30-60).

Regarding claim 91, Candelore discloses a recordable medium having recorded thereon a reordered content item resulting from the process comprising:

storing an original content item as multiple blocks, each block containing at least a single byte col. 19, lines 44-67 and col. 20, lines 1-5), generating a key in response to [an identifier value of a content retrieval entity](col. 24, lines 66-67 and col. 25, lines 1-20)(col. 26, lines 45-60 – wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit), and reordering, as controlled by the key (i.e., address data signal), blocks of an original content item to create the reordered content item (i.e., a block-wise scrambling of N blocks according to an address data signal)(col. 26, lines 14-30), wherein the re-ordered blocks are stored in a non-linear fashion within the storage allocated for the re-ordered content item (col. 23, lines 63-67 and col. 24, lines 1-5).

Regarding claims 2-4, Candelore discloses the apparatus of claim 1 further comprising: a transmitter to distribute the reordered blocks over a wireless broadcast channel (col. 2, lines 38-60).

Regarding claim 5, Candelore discloses further comprising: means for writing the reordered blocks to a removable storage disc (col. 1, lines 50-67 and col. 2, lines 1-7 and col. 23, lines 30-36).

Regarding claim 6, Candelore discloses the apparatus of claim 1 further comprising:

a storage to store the reordered blocks using an addressing scheme that is the same as the one used to store the original content item, reordered blocks stored orthogonal to the addressing scheme (col. 26, lines 45-60).

Regarding claim 7, Candelore discloses wherein each of the reordered blocks comprises a same data content as its corresponding block from the original content item (i.e., each of the re-ordered blocks contain the same original content item before they get encrypted in the encryption/decryption circuit 120)(col. 19, lines 35-64).

Regarding claims 8-9, Candelore discloses wherein the reordered blocks are of any block sizes (col. 22, lines 17-38).

Regarding claims 21-26, Candelore discloses wherein the original content item comprises an electronic programming guide (col. 2, lines 39-50).

Regarding claims 27-28, Candelore discloses an apparatus that further comprises a storage device, and wherein the reorderer conventionally encrypts the blocks of the original content item, reorders blocks of the original content item and stores them to the storage device according to a logical addressing system of the apparatus (col. 23, lines 30-36 and col. 26, lines 45-60).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-20, 80-81, and 92-96 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore et al., (U.S. Patent No. 6,061,449 and Candelore hereinafter), in view of Etzel et al., (U.S. Patent No. 6,577,734 and Etzel hereinafter).

Regarding claims 10-11, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit (col. 25, lines 5-20).

Moreover, Etzel discloses further comprising: a storage to store a list of identifier values of a plurality of such other apparatuses (i.e., database of CV keys) wherein, for different identifier values of two such other apparatuses (col. 7, lines 7-21), the key generator generates different keys, and wherein, in response to the different keys (i.e., a security module, e.g., module 30, generates a shared symmetrical encryption key with another security module, e.g., security module 50), the reorderer (i.e., security module)

[imposes different new block orders on the original content item] (col. 4, lines 55-67 and col. 5, lines 1-7 and col. 6, lines 19-42).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include a storage to store a list of identifier values of a plurality of such other apparatuses to use such identifiers in a device-specific video information delivery system as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claim 12, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit. Candelore further discloses the scrambling sender scrambles the sequence of the blocks before transmitting them to the descrambling receiver (col. 25, lines 5-20).

Etzel discloses a list including a first identifier value for a first such other apparatus, and a second identifier value for both a second and a third such other apparatus, wherein the second identifier value is different than the first identifier value (i.e., CV is a function of the address of the associated subscriber terminal)(col. 6, lines 3-42), and the reorderer (i.e., security module) [imposes a first new block order on the

original content item for distribution to the first such other apparatus, and a second, different new block order on the original content item for distribution to either the second or the third such other apparatus] (col. 6, lines 46-67 and col. 7, lines 45-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include identifiers in a device-specific video information delivery system as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claims 13-16, and 94-96, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit (col. 25, lines 5-20).

Etzel discloses wherein the identifier value is a serial number of the other apparatus (col. 4, lines 38-55 and col. 8, lines 5-17).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include using serial numbers as identifiers in a device- specific video information delivery system as disclosed by Etzel. This

modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claim 17, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit. Candelore further discloses the scrambling sender scrambles the sequence of the blocks before transmitting them to the descrambling receiver (col. 25, lines 5-20 and col. 26, lines 45-60).

Etzel discloses wherein: the apparatus is a server, the other apparatus is one of a plurality of clients, and the server further comprises, means for provisioning the clients, including the selection of the identifier values for the clients (i.e., only the terminals whose address is contained in the message "reads in" the message), and means for maintaining a list of the clients' identifier values (i.e., module 215 locates the program id in the message, associates that id with the proper key-cache memory location, unloads the program encryption key stored at that memory location, and uses the key to decrypt the program segment contained in the received message)(col. 7, lines 45-67 and col. 8, lines 1-5).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of

Etzel because it would allow to expressly include device-specific identifiers in a device-specific video information delivery to a plurality of client devices as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claim 18, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit (col. 25, lines 5-20).

Etzel discloses wherein the identifier value comprises the session key (i.e., the video on demand system)(col. 2, lines 29-39).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include session keys in a device-specific video information delivery to a plurality of client devices in a VOD-enabled system as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claims 19-20, Candelore further discloses the scrambling sender scrambles the sequence of the blocks before transmitting them to the descrambling receiver (col. 26, lines 45-60).

Etzel discloses a transmitter for communicating over a key channel and a content channel (i.e., wherein the bi-directional communication path 41 and the uni-direction path 61 are the physical channels including the virtual channels for transmitting key and content)(col. 7, lines 4-6 and lines 45-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include communicating over a key channel and a content channel as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claims 80-81, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit. (col. 25, lines 5-20).

Etzel discloses generating a local key within the second entity, [in response to which the block reordering structure is created] (i.e., a respective symmetrical key is

unique to the pair of module as a result of the public key associated with the receiving module/module 215)(col. 4, lines 55-67 and col. 5, lines 1-7).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include device-specific identifiers in a device-specific video information delivery to a plurality of client devices as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claim 92, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit. Candelore further discloses the scrambling sender scrambles the sequence of the blocks before transmitting them to the descrambling receiver (col. 25, lines 5-20 and col. 26, lines 45-60).

Etzel discloses wherein the reordered content item results from the process further comprising: the process being performed in a server, and the content retrieval entity being one of a plurality of clients connectable to the server, and the server maintaining a list of respective identifier values of the clients (col. 6, lines 19-42 and col. 7, lines 7-28).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of Etzel because it would allow to expressly include device-specific identifiers in a device-specific video information delivery to a plurality of client devices as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Regarding claim 93, Candelore discloses wherein unit-dependent keys are used to prevent a pirate from using the key or keys obtained from one unit to either encrypt, encrypt and authenticate, or authenticate program information for another unit. Candelore further discloses the scrambling sender scrambles the sequence of the blocks before transmitting them to the descrambling receiver (col. 25, lines 5-20 and col. 26, lines 45-60).

Etzel discloses wherein the reordered content item results from the process further comprising: the server creating the respective identifier values of the clients to be mutually unique (i.e., a respective symmetrical key is unique to the pair of module as a result of the public key associated with the receiving module/module 215)(col. 4, lines 55-67 and col. 5, lines 1-7).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Candelore with teachings of

Etzel because it would allow to expressly include device-specific identifiers in a device-specific video information delivery to a plurality of client devices as disclosed by Etzel. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Etzel to prevent illicit production of a service provider's decryption key, thereby disallowing a person to fraudulently an encrypted video program (Candelore, col. 1, lines 30-40).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
April 3/2007

CHRISTOPHER REVAK
PRIMARY EXAMINER